

SOLUTIONS OF A LINEAR EQUATION IN A SUBGROUP OF UNITS IN A FUNCTION FIELD

CHIA-LIANG SUN

- Institute of Mathematics, Academia Sinica
E-mail: `csun@math.sinica.edu.tw`

ABSTRACT. Over a large class of function fields, we show that the solutions of some linear equations in the topological closure of a certain subgroup of the group of units in the function field are exactly the solutions that are already in the subgroup. This result solves some cases of the function field analog of an old conjecture proposed by Skolem.

1. INTRODUCTION

Let K/k be a function field, i.e., K is finitely generated over k with transcendence degree 1 such that k is relatively algebraically closed in K . Let $\Omega_{K/k}$ be the set of all places of K/k . Let M be a natural number, and \mathbb{A}^M be the affine M -space, whose coordinate is denoted by $\mathbf{X} = (X_1, \dots, X_M)$. For any two elements $\mathbf{a} = (a_1, \dots, a_M)$ and $\mathbf{b} = (b_1, \dots, b_M)$ in $\mathbb{A}^M(K^*)$, we define $\mathbf{a}\mathbf{b} = (a_1b_1, \dots, a_Mb_M) \in \mathbb{A}^M(K)$ and $\mathbf{a} \cdot \mathbf{b} = \sum_{i=1}^M a_i b_i \in K$; we also write $\mathbf{b} \cdot \mathbf{X}$ for the function $\sum_{i=1}^M b_i X_i$ on \mathbb{A}^M . For any subset Θ of some ring and any variety V in \mathbb{A}^M , let $V(\Theta)$ denote the set of points on V with each coordinate in Θ . For any $\mathbf{b} \in \mathbb{A}^M(K^*)$, we denote by $W_{\mathbf{b}}$ (resp. $W'_{\mathbf{b}}$) the variety in \mathbb{A}^M defined by $\mathbf{b} \cdot \mathbf{X} = 0$ (resp. $\mathbf{b} \cdot \mathbf{X} = 1$). We fix a cofinite subset $\Omega \subset \Omega_{K/k}$ and endow $\prod_{v \in \Omega} K_v^*$ with the natural product topology. Via the diagonal embedding, we identify any subgroup $\Gamma \subset K^*$ with its image in $\prod_{v \in \Omega} K_v^*$, and denote by $\bar{\Gamma}$ its topological closure. Moreover, for each $v \in \Omega_{K/k}$, the inclusion $\Gamma \subset K_v^*$ is continuous and therefore induces a subtopology of Γ , which will be referred to as *v-adic subtopology*.

The purpose of this paper is investigate the circumstances where the equalities

$$(1) \quad W_{\mathbf{b}}(\bar{\Gamma}) = W_{\mathbf{b}}(\Gamma)$$

$$(2) \quad W'_{\mathbf{b}}(\bar{\Gamma}) = W'_{\mathbf{b}}(\Gamma)$$

hold. In the case where $M = 1$, both sides of (1) are always empty; however, Example 0 in [Sun] shows that (2) may fail unless we make some restrictions on the largeness of Γ . In the characteristic zero case, this is indeed the only assumption needed.

Theorem 1. *Suppose that k has characteristic 0. Let $\Gamma \subset K^*$ be a subgroup contained in O_S^* for some finite $S \subset \Omega_{K/k}$. Then for any $v \in \Omega_{K/k}$, the v -adic subtopology of Γ is discrete. In particular, both (1) and (2) hold.*

In the case where k is finite, the main result in [Sun] shows that (2) holds if $M = 1$ and Γ is finitely generated. Nevertheless, Example 1 suggests that even in the case where $M = 2$, both (1) and (2) can fail in general, unless we put some

mixed assumptions on \mathbf{b} and Γ . Recall that K is *separably generated* over k if there exists $t \in K$ such that K is finite separable over $k(t)$. The separable Hilbert subset $H_k(f_1, \dots, f_m; g)$ of k , where each $f_i(T, X)$ is a separable irreducible polynomial in $k(T)[X]$ and $g(T)$ is a nonzero polynomial in $k[T]$, consists of those $a \in k$ such that $g(a) \neq 0$ and each $f_i(a, X)$ is defined and irreducible in $k[X]$ [FJ08]. For each i , let $\psi_i : \mathbb{A}^M(K^*) \rightarrow \mathbb{A}^M(K^*)$ be the map which replaces the i -th component of $\mathbf{a} \in \mathbb{A}^M(K^*)$ by 1 and keeps the others unchanged. We shall prove the following result.

Theorem 2. *Suppose that k has characteristic p , and either*

- *that k is finite, or*
- *that K is separably generated over k , that each separable Hilbert subset of k is infinite, and that k contains only finitely many roots of unity.*

Let $\mathbf{b} \in \mathbb{A}^M(K^)$ be contained in $\mathbb{A}^M(O_S^*)$ for some finite $S \subset \Omega_{K/k}$, and $\Gamma \subset O_S^*$ be a subgroup. For each natural number m , let $R_m \subset \Gamma$ be a complete set of representatives of $\Gamma/\Gamma \cap (kK^{p^m})^*$.*

- (1) *Each R_m is a finite set.*
- (2) *Suppose that there is some m such that for every $\mathbf{r} \in \mathbb{A}^M(R_m)$ the components of \mathbf{br} are linearly independent over kK^{p^m} . Then both sides of (1) are empty.*
- (3) *Suppose that there is some m such that for every $\mathbf{r} \in \mathbb{A}^M(R_m)$ the components of some $\psi_j(\mathbf{br})$ are linearly independent over kK^{p^m} . Then (2) holds, and the common set is finite with its cardinality no larger than the number of $\mathbf{r} \in \mathbb{A}^M(R_m)$ such that the components of \mathbf{br} and those of each $\psi_j(\mathbf{br})$ are linearly independent over kK^{p^m} .*

A large class of fields satisfy the assumption of Theorem 2 on k . In fact, if k is a global field, then each separable Hilbert subset of k is infinite ([FJ08], Theorem 13.3.5) and k contains only finitely many roots of unity; these two properties are preserved under a purely transcendental extension with arbitrary cardinality as its transcendence degree (*op. cit.*, Proposition 13.2.1) and any algebraic extension with a finite separable degree (*op. cit.*, Proposition 12.3.3).

Some brief remarks on the hypotheses of Theorem 2 follow. In case where $M = 1$, the assumptions in (2) and (3) are vacuous. When k is finite and $M = 2$, using Lemma 3 in [Vol98], we may replace the assumption in (2) with $b_1 b_2^{-1} \notin \sqrt{\Gamma}$, and that in (3) with $\{b_1, b_2\} \not\subset \sqrt{\Gamma}$, where $\sqrt{G} = \{x \in K^* : x^n \in G \text{ for some } n \in \mathbb{N}\}$ for any subgroup $G \subset K^*$.

Example 1. Let $K = \mathbb{F}_p(t)$ be a purely transcendental extension of \mathbb{F}_p , and $\Gamma = \langle t, -t, 1-t \rangle$ be the subgroup of K^* generated by t , $-t$, and $1-t$. Take $\Omega \subset \Omega_K$ to be a cofinite subset such that Γ is contained in the valuation ring O_v for every $v \in \Omega$, and $\mathbf{b} = (1, 1) \in \mathbb{A}^2(K^*)$. The sequence $(t^{p^{n!}})_{n \geq 1}$ in Γ converges to $\alpha \in \overline{\Gamma} \setminus K^*$ ([Sun], Example 1). Therefore we see that $(\alpha, -\alpha) \in W_{\mathbf{b}}(\overline{\Gamma}) \setminus W_{\mathbf{b}}(\Gamma)$ and $(\alpha, 1-\alpha) \in W'_{\mathbf{b}}(\overline{\Gamma}) \setminus W'_{\mathbf{b}}(\Gamma)$.

In case where $\Gamma \subset O_S^*$ and $\mathbf{b} \in \mathbb{A}^M(O_S^*)$ for some finite $S \subset \Omega_{K/k}$, the equalities (1) and (2) are stronger assertions than the function field analog of an old conjecture raised by Skolem [Sko37]. To state his conjecture, we make the following

abbreviation:

$\mathfrak{S}_L(K/k, M, \mathbf{b}, S, \Gamma)$ stands for For each nonzero ideal $I \subset O_S$ there exists $\mathbf{x} \in \mathbb{A}^M(\Gamma)$ such that $\mathbf{b} \cdot \mathbf{x} \in I$.

$\mathfrak{S}_G(K/k, M, \mathbf{b}, S, \Gamma)$ stands for There exists $\mathbf{x} \in \mathbb{A}^M(\Gamma)$ such that $\mathbf{b} \cdot \mathbf{x} = 0$.

In the case where K is a number field and S contains all Archimedean places, Skolem asserts that $\mathfrak{S}_L(K, M, \mathbf{b}, S, \Gamma) \Leftrightarrow \mathfrak{S}_G(K, M, \mathbf{b}, S, \Gamma)$ should always hold, and gives a proof when $M = 2$ [Sko37]. The validity of Skolem's assertion seems to have been largely ignored in the recent literature until Harari and Voloch [HV10] noticed its connection with (1) and (2). In fact, we may translate Theorem 1 and Theorem 2 into results on Skolem's conjecture via the following equivalences:

$$\begin{aligned} \mathfrak{S}_L(K/k, M, \mathbf{b}, S, \Gamma) &\Leftrightarrow W_{\mathbf{b}}(\bar{\Gamma}) \neq \emptyset \Leftrightarrow W'_{\phi_i(\mathbf{b})}(\bar{\Gamma}) \neq \emptyset \quad \text{where } \Omega = \Omega_{K/k} \setminus S \\ \mathfrak{S}_G(K/k, M, \mathbf{b}, S, \Gamma) &\Leftrightarrow W_{\mathbf{b}}(\Gamma) \neq \emptyset \Leftrightarrow W'_{\phi_i(\mathbf{b})}(\Gamma) \neq \emptyset \end{aligned}$$

for each i , where $\phi_i : \mathbb{A}^M(K^*) \rightarrow \mathbb{A}^{M-1}(K^*)$ is defined by

$$(a_1, \dots, a_M) \mapsto \left(-\frac{a_1}{a_i}, \dots, -\frac{a_{i-1}}{a_i}, -\frac{a_{i+1}}{a_i}, \dots, -\frac{a_M}{a_i} \right).$$

For instance, if K/k satisfies the assumptions in Theorem 2, then $\mathfrak{S}_L(K/k, 2, \mathbf{b}, S, \Gamma) \Leftrightarrow \mathfrak{S}_G(K/k, 2, \mathbf{b}, S, \Gamma)$ always holds.

2. PROOF OF THE MAIN RESULTS

Lemma 1. *Let $\Gamma \subset K^*$ be a subgroup contained in O_S^* for some finite $S \subset \Omega_{K/k}$. Then for any $v \in \Omega_{K/k}$, there is a subgroup $G_v \subset \Gamma$ which is open in the v -adic subtopology. If we further suppose that k contains only finitely many roots of unity, then G_v may be chosen such that $\sqrt{G_v}$ is finitely generated.*

Proof. Taking $G_v = \Gamma \cap (1 + m_v)$, we see that G_v is open in the v -adic subtopology of Γ since $1 + m_v$ is an open subgroup of K_v^* . The inclusion $\Gamma \subset O_S^*$ induces the map $G_v \rightarrow O_S^*/k^*$, which is injective because $k^* \cap (1 + m_v)$ is trivial. The first conclusion follows from the fact that O_S^*/k^* is finitely generated (Corollary 1 of Proposition 14.1, [Ros02]). Now we show that $\sqrt{G_v}$ is finitely generated under the additional hypothesis that k contains only finitely many roots of unity. Note that $\sqrt{G_v} \subset \sqrt{\Gamma} \subset O_S^*$, which again induces the map $\sqrt{G_v} \rightarrow O_S^*/k^*$ with its kernel contained in $k^* \cap \sqrt{K^* \cap (1 + m_v)}$, which is exactly the group of roots of unity in k . This completes the proof. \square

Proof of Theorem 1: Fix $v \in \Omega_{K/k}$ and let $U_n = \Gamma \cap (1 + m_v^n)$ for $n \geq 1$. Then U_n is open in the v -adic subtopology of Γ . Since k has characteristic zero, the quotient groups U_n/U_{n+1} are torsion-free for all n . The proof of Lemma 1 shows that U_1 is finitely generated, hence U_n is trivial for some n . \square

Lemma 2. *Suppose that K is separably generated over k , and that each separable Hilbert subset of k is infinite. Let L be a finite separable extension of K . Then there are infinitely many $v \in \Omega_{K/k}$ which extend uniquely and unramifiedly to a place of L .*

Proof. Since K is separably generated over k , it is enough to assume that $K = k(t)$, in which case the desired property follows from the infiniteness of the separable Hilbert subset $H_k(f; 1)$, where $L = K(y)$ with y a root of the separable polynomial $f \in k(T)[X]$. \square

Lemma 3. *Suppose that K/k satisfies the assumptions in Theorem 2. Let $\Gamma \subset K^*$ be a subgroup contained in O_S^* for some finite $S \subset \Omega_{K/k}$. Then for any integer m prime to p , the subgroup Γ^m of Γ is open.*

Proof. The case where k is finite is proved in Lemma 12 of [Sun]. Thus we assume that k is infinite. By Lemma 1, we may assume that $\sqrt{\Gamma}$ is finitely generated; then by Lemma 5 of [Sun], we may further assume that $\Gamma = \sqrt{\Gamma}$. Let L be the finite Galois extension of K obtained by adjoining all the m -th roots of every element in Γ . For each field E such that $K \subset E \subset L$, Lemma 2 yields a place $v_E \in \Omega$ which extends to a unique place v_E of E such that $[E_{v_E} : K_{v_E}] = [E : K]$. Let S be the finite set consisting of those v_E such that there is no proper intermediate field between K and E . We shall complete the proof by showing that $\Gamma \cap U_S \subset \Gamma^m$, where $U_S = \prod_{v \in S} 1 + m_v$ is an open subgroup of $\prod_{v \in S} K_v^*$. In fact, we only have to show that $\Gamma \cap U_S \subset (K^*)^m$ because $\Gamma = \sqrt{\Gamma}$. Assume $x \in \Gamma \cap U_S \setminus (K^*)^m$ and let F be the extension of K obtained by adjoining an m -th root of x . Then we have $K \subsetneq E \subset F \subset L$ for some E such that $v_E \in S$. Since $[E_{v_E} : K_{v_E}] = [E : K] \neq 1$, it follows that x has no m -th root in K_{v_E} , which contradicts the assumption $x \in U_S$ by Hensel's lemma. \square

Lemma 4. *Suppose that k has characteristic p , and that k contains only finitely many roots of unity. Let $\Gamma \subset K^*$ be a subgroup contained in O_S^* for some finite $S \subset \Omega_{K/k}$. Then for every $v \in \Omega_{K/k}$, any subgroup of Γ containing Γ^{p^n} for some $n \in \mathbb{N}$ is open in the v -adic subtopology of Γ .*

Proof. It suffices to show that those subgroups Γ^{p^n} are open in the v -adic subtopology of Γ . As in the proof of Lemma 3, we may assume that $\Gamma = \sqrt{\Gamma}$ is finitely generated. Because $(K_v^*)^{p^n} \cap K^* = (K^*)^{p^n}$, we have $(K_v^*)^{p^n} \cap \Gamma \leq (K^*)^{p^n} \cap \Gamma = \Gamma^{p^n}$. Then it suffices to show that $(K_v^*)^{p^n} \cap \Gamma$ is open in the v -adic subtopology of Γ . Note that $(K_v^*)^{p^n}$ is closed in K_v^* and consequently $K_v^*/(K_v^*)^{p^n}$ is Hausdorff. Consider the map $\Gamma \rightarrow K_v^*/(K_v^*)^{p^n}$ induced from the inclusion $\Gamma \subset K_v^*$, which is continuous with respect to the v -adic subtopology of Γ . Since this map factors through Γ/Γ^{p^n} , its image is finite, whence discrete. This completes our proof. \square

Corollary 1. *Suppose that K/k satisfies the assumptions in Theorem 2. Let $\Gamma \subset K^*$ be a subgroup contained in O_S^* for some finite $S \subset \Omega_{K/k}$. Then any subgroup of Γ containing Γ^m for some $m \in \mathbb{N}$ is open.* \square

Corollary 2. *Suppose that K/k satisfies the assumptions in Theorem 2. Let $\Gamma \subset K^*$ be a subgroup contained in O_S^* for some finite $S \subset \Omega_{K/k}$. Then Γ is closed in K^* .*

Proof. Let $P \in \overline{\Gamma} \cap K^*$. Lemma 1 (and its proof) shows that $P \in \overline{\Gamma_0}$ for some finitely generated subgroup $\Gamma_0 \subset \Gamma$ such that Γ_0 is contained in a finitely generated closed subgroup $\Gamma_S \subset O_S^*$. By enlarging S , we may assume $S \cup \Omega = \Omega_{K/k}$ and hence both O_S^* and Γ_S are closed in K^* . By Corollary 1, every subgroup of Γ_S with finite index is open; hence Γ_0 is closed in Γ_S , and thus in K^* . This shows $P \in \Gamma_0 \subset \Gamma$ and finishes our proof. \square

Corollary 3. *Suppose that K/k satisfies the assumptions in Theorem 2. Let $\Gamma \subset K^*$ be a subgroup contained in O_S^* for some finite $S \subset \Omega_{K/k}$. Then for any subgroup Δ of Γ containing Γ^m for some $m \in \mathbb{N}$, the homomorphism*

$$\Gamma/\Delta \rightarrow \overline{\Gamma}/\overline{\Delta}$$

is bijective.

Proof. By Corollary 2, we have $\Gamma \cap \overline{\Delta} = \Gamma \cap (\overline{\Delta} \cap K^*) = \Delta$, which is the desired injectivity. By Corollary 1, Δ is open in Γ , hence the desired surjectivity follows. (c.f. Lemma 8, [Sun]) \square

Lemma 5. *Suppose that k has positive characteristic p , and that K is separably generated over k . Then for any $n > 0$, we have $K \cap \overline{k}K^{p^n} = kK^{p^n}$.*

Proof. Denote by k^{sep} the separable closure of k in \overline{k} . As $K \cap k^{\text{sep}}K^{p^n}$ is both separable and purely inseparable over kK^{p^n} , they are equal to each other; hence it remains to show that $K \cap \overline{k}K^{p^n} \subset k^{\text{sep}}K^{p^n}$. Let $K = k(t, y)$ with y separable over $k(t)$. Then $K = k(t, y^{p^n})$ and thus $K \cap \overline{k}K^{p^n} = k(t, y^{p^n}) \cap \overline{k}(t^{p^n}, y^{p^n}) \subset k^{\text{sep}}(t, y^{p^n}) \cap \overline{k}(t^{p^n}, y^{p^n})$. The irreducible polynomial of y^{p^n} over $k^{\text{sep}}(t)$ is still irreducible over $\overline{k}(t)$, and therefore $k^{\text{sep}}(t, y^{p^n}) \cap \overline{k}(t^{p^n}, y^{p^n}) = k^{\text{sep}}(t^{p^n}, y^{p^n})$ since $k^{\text{sep}}(t) \cap \overline{k}(t^{p^n}) = k^{\text{sep}}(t^{p^n})$. This completes the proof. \square

Lemma 6. *Suppose that k has positive characteristic p , and that K is separably generated over k . Then for each $v \in \Omega_{K/k}$ and each $n > 0$, any kK^{p^n} -linear map $\phi : K \rightarrow K$ is continuous with respect to the v -adic topology.*

Proof. Any $v \in \Omega_{K/k}$ gives a discrete valuation $v : K^* \rightarrow \mathbb{Z}$ such that $v(s) = 1$ for some $s \in K^*$ and that $v((kK^{p^n})^*) \subset p^n\mathbb{Z}$. It follows that $\{s^j\}_{0 \leq j \leq p^n-1}$ is K^{p^n} -linearly independent. Since K is separably generated over k , we have $[K : kK^{p^n}] = p^n$ and conclude that $\{s^j\}_{0 \leq j \leq p^n-1}$ is a K^{p^n} -linear basis for K . To prove this lemma, it is enough to show the continuity of ϕ at 0. Let $x = \sum_{j=0}^{p^n-1} c_j s^j \neq 0$ with all $c_j \in kK^{p^n}$. Then $v(x) = \min_{c_j \neq 0} (v(c_j) + j)$ and $\phi(x) = \sum_{j=0}^{p^n-1} c_j \phi(s^j)$. Thus, we have $v(\phi(x)) \geq \min_{c_j \neq 0} (v(c_j) + v(\phi(s^j))) \geq v(x) + \min_{0 \leq j \leq p^n-1} (v(\phi(s^j) - s^j))$. This finishes the proof since $\min_{0 \leq j \leq p^n-1} (v(\phi(s^j) - s^j))$ is independent of x . \square

For each $v \in \Omega_{K/k}$ and each natural number m , denote by $(kK^{p^m})_v^*$ the topological closure of $(kK^{p^m})^*$ in K_v^* .

Proposition 1. *Suppose that k has positive characteristic p , and that K is separably generated over k . Let $\mathbf{b} \in (K^*)^M$, and let m be a natural number.*

- a) *Suppose that the components of \mathbf{b} are linearly independent over kK^{p^m} . Then we have*

$$W_{\mathbf{b}} \left((kK^{p^m})_v^* \right) = \emptyset \quad \text{for all } v \in \Omega_{K/k}.$$

- b) *Suppose that for some j the components of $\psi_j(\mathbf{b})$ are linearly independent over kK^{p^m} . Then for some $P \in W'_{\mathbf{b}}(K)$ we have*

$$\prod_{v \in \Omega_{K/k}} W'_{\mathbf{b}} \left((kK^{p^m})_v^* \right) \subset \{P\}.$$

If, moreover, the components of either \mathbf{b} or some $\psi_l(\mathbf{b})$ are linearly dependent over kK^{p^m} , then we have

$$W'_{\mathbf{b}} \left((kK^{p^m})_v^* \right) = \emptyset \quad \text{for all } v \in \Omega_{K/k}.$$

Proof. Choose $t \in \bar{k}K$ such that $\bar{k}(t) \subset \bar{k}K \subset \bar{k}((t))$. By Remark 1 in [GV87], there exists an iterative derivation $\{D_{\bar{k}K}^{(i)}\}_{i \geq 0}$ on $\bar{k}K$ such that $\bar{k}K^{p^m} = \{x \in \bar{k}K : D_{\bar{k}K}^{(l)}(x) = 0, \text{ if } 1 \leq l < p^m\}$ for $i, j \geq 0$. Taking restriction gives an iterative derivation $\{D_K^{(i)}\}_{i \geq 0}$ on K such that $\{x \in K : D_K^{(l)}(x) = 0, \text{ if } 1 \leq l < p^m\} = K \cap \bar{k}K^{p^m} = kK^{p^m}$ by Lemma 5. By Lemma 6, for each $v \in \Omega_{K/k}$, we extend each $\{D_K^{(i)}\}_{i \geq 0}$ to an iterative derivation $\{D_{K_v}^{(i)}\}_{i \geq 0}$ on K_v by continuity, and note that $D_{K_v}^{(i)}|_{((kK^{p^m})^*)_v}$ is the zero map for any $1 \leq i < p^m$.

Fix some $v \in \Omega_{K/k}$ and some $\mathbf{c} = (c_1, \dots, c_M) \in W_{\mathbf{b}}((kK^{p^m})^*)_v \cup W'_{\mathbf{b}}((kK^{p^m})^*)_v$. Then $\sum_{j=1}^N b_j c_j = e$, where $e \in \{0, 1\}$. For any $0 \leq i < p^m$, because $D_{K_v}^{(i)}(c_j) = 0$, we have that

$$(3) \quad \sum_{j=1}^N D_K^{(i)}(b_j) c_j^{(l)} = D_K^{(i)}(e).$$

Denote by \mathbf{c} (resp. \mathbf{e}) the M -by-1 matrix with the j -th component c_j (resp. $D_K^{(j)}(e)$). For any set $I = \{i_1, \dots, i_M\}$ of M nonnegative integers such that $0 = i_1 < i_2 < \dots < i_M < p^m$, let $\mathbf{T}_{\mathbf{b}, I}$ be the M -by- M matrix with the entry $D_K^{(i_l)}(b_j)$ being at the l -th row and j -th column. From (3), we have $\mathbf{T}_{\mathbf{b}, I} \mathbf{c} = \mathbf{e}$, which implies

$$(4) \quad (\det \mathbf{T}_{\mathbf{b}, I}) \mathbf{c} = \mathbf{T}_{\mathbf{b}, I}^* \mathbf{e},$$

where $\mathbf{T}_{\mathbf{b}, I}^*$ denotes the adjoint matrix of $\mathbf{T}_{\mathbf{b}, I}$. If $e = 0$ and the components of \mathbf{b} are linearly independent over kK^{p^m} , then by Theorem 1 of [GV87], $\det \mathbf{T}_{\mathbf{b}, I} \neq 0$ for some I , which contradicts $\mathbf{c} \neq 0$. This proves (a).

To prove (b), we consider the case where $e = 1$. Note that the j -th component of $\mathbf{T}_{\mathbf{b}, I}^* \mathbf{e}$ is exactly $\det \mathbf{T}_{\psi_j(\mathbf{b}), I}$. Under the assumption in the first part, Theorem 1 of [GV87] implies that $\det \mathbf{T}_{\psi_j(\mathbf{b}), I} \neq 0$ for some j and I . Hence there is at most one choice for \mathbf{c} satisfying (4), and this choice gives $P \in W'_{\mathbf{b}}(K)$. If the additional hypothesis also holds, then either $\det \mathbf{T}_{\mathbf{b}, I}$ or some component of $\mathbf{T}_{\mathbf{b}, I}^* \mathbf{e}$ is zero, and (4) is impossible. \square

Proof of Theorem 2. First, note that for each m the kernel of the natural map

$$\Gamma \rightarrow (O_S^*/k^*) / (O_S^*/k^*)^m$$

is contained in $(kK^{p^m})^*$. This proves (1) since O_S^*/k^* is finitely generated (Corollary 1 of Proposition 14.1, [Ros02]). We have

$$\bar{\Gamma} = \bigcup_{\gamma \in R_m} \gamma \bar{\Gamma} \cap (kK^{p^m})^* \subset \bigcup_{\gamma \in R_m} \prod_{v \in \Omega} \gamma (kK^{p^m})^*_v,$$

where the first equality follows from Corollary 3. This gives

$$W_{\mathbf{b}}(\bar{\Gamma}) \subset \prod_{v \in \Omega} W_{\mathbf{b}} \left(\bigcup_{\gamma \in R_m} \gamma (kK^{p^m})^*_v \right) = \bigcup_{\mathbf{r} \in \mathbb{A}^M(R_m)} \prod_{v \in \Omega} \mathbf{r} W_{\mathbf{b}\mathbf{r}}((kK^{p^m})^*_v).$$

Proposition 1(a) shows that $\prod_{v \in \Omega} W_{\mathbf{b}\mathbf{r}}((kK^{p^m})^*_v) = \emptyset$ for each $\mathbf{r} \in \mathbb{A}^M(R_m)$, proving (2).

Similarly, we have

$$W'_{\mathbf{b}}(\bar{\Gamma}) \subset \bigcup_{\mathbf{r} \in \mathbb{A}^M(R_m)} \prod_{v \in \Omega} \mathbf{r} W'_{\mathbf{b}\mathbf{r}}((kK^{p^m})^*_v).$$

Let $U \subset \mathbb{A}^M(R_m)$ be the subset consisting of those \mathbf{r} such that the components of \mathbf{br} and those of each $\psi_j(\mathbf{br})$ are linearly independent over kK^{p^m} . By Proposition 1(b), for each $\mathbf{u} \in U$ there exists some $P_{\mathbf{u}} \in W'_{\mathbf{bu}}(K)$ such that $\prod_{v \in \Omega} W'_{\mathbf{br}}((kK^{p^m})_v^*) \subset \{P_{\mathbf{u}}\}$, while for each $\mathbf{r} \in R^M \setminus \mathbb{A}^M(R_m)$, we have $\prod_{v \in \Omega} W'_{\mathbf{br}}((kK^{p^m})_v^*) = \emptyset$. Then, $W'_{\mathbf{b}}(\bar{\Gamma}) \subset \{\mathbf{u}P_{\mathbf{u}} : \mathbf{u} \in U\} \subset W'_{\mathbf{b}}(K)$. It follows that $W'_{\mathbf{b}}(\bar{\Gamma}) \subset W'_{\mathbf{b}}(\bar{\Gamma}) \cap W'_{\mathbf{b}}(K) = W'_{\mathbf{b}}(\bar{\Gamma} \cap K^*) = W'_{\mathbf{b}}(\Gamma)$, where the last equality is concluded by Corollary 2. This finishes our proof. \square

REFERENCES

- [FJ08] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, third edition, 2008. Revised by M. Jarden.
- [GV87] Arnaldo García and J. F. Voloch. Wronskians and linear independence in fields of prime characteristic. *Manuscripta Math.*, 59(4):457–469, 1987.
- [HV10] David Harari and José Felipe Voloch. The Brauer-Manin obstruction for integral points on curves. *Math. Proc. Cambridge Philos. Soc.*, 149(3):413–421, 2010.
- [Ros02] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.
- [Sko37] Thoralf Skolem. Anwendung exponentieller Kongruenzen zum Beweis der Unlösbarkeit gewisser diophantischer Gleichungen. *Avhdl. Norske Vid. Akad. Oslo I*, 12:1–16, 1937.
- [Sun] Chia-Liang Sun. Product of local points of subvarieties of almost isotrivial semi-abelian varieties over a global function field. preprint arXiv.
- [Vol98] José Felipe Voloch. The equation $ax + by = 1$ in characteristic p . *J. Number Theory*, 73(2):195–200, 1998.